(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2004 (05.02.2004)

PCT

(10) International Publication Number
WO 2004/012384 A2

(51) International Patent Classification[7]: H04L 9/06

(21) International Application Number:
PCT/US2003/023473

(22) International Filing Date: 25 July 2003 (25.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/399,092 27 July 2002 (27.07.2002) US

(71) Applicant and
(72) Inventor: HOTZ, Jimmy, Christian [US/US]; 3094 Fort Courage Avenue, Thousand Oaks, CA 91360 (US).

(74) Agents: RITCHIE, David, B. et al.; THELEN REID & PRIEST LLP, P.O. BOX 640640, San Jose, CA 95164-0640 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

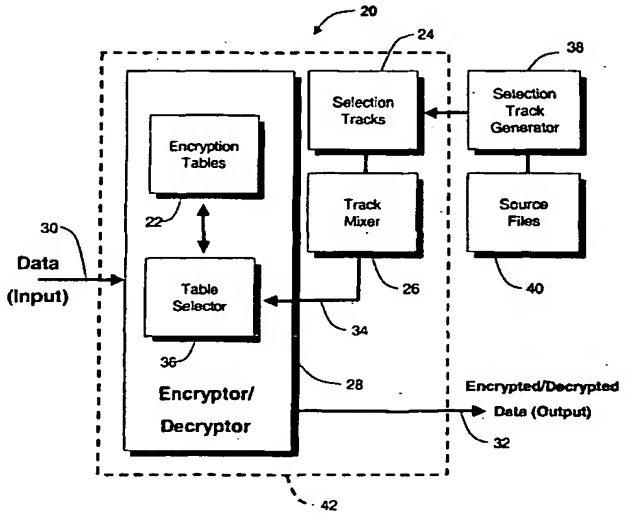
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: APPARATUS AND METHOD FOR ENCTYPTION AND DECRYPTION



(57) Abstract: An apparatus and method for encrypting/decrypting data include (a) a first plurality of encryption tables, each of the encryption tables being capable of transforming a data value into an encrypted/decrypted value, the data value corresponding to a unit of the data, the encrypted/decrypted value corresponding to a unit of encrypted/decrypted data, (b) a second plurality of selection tracks, each of the selection tracks including a series of values having a certain pattern, (c) a track mixer coupled to the second plurality of selection tracks, adapted to combine corresponding values of the selection tracks to produce a series of combined values, and (d) an encryption/decryption module coupled to the first plurality of encryption tables and the track mixer, adapted to transform each unit of the data into a unit of encrypted/decrypted data using an encryption table selected for that unit according to a combined value in the series of combined values.

WO 2004/012384 A2